iSpirit 4504 交换机快速配置指南

(软件版本：主控 1v24，24 口模块 1v211)

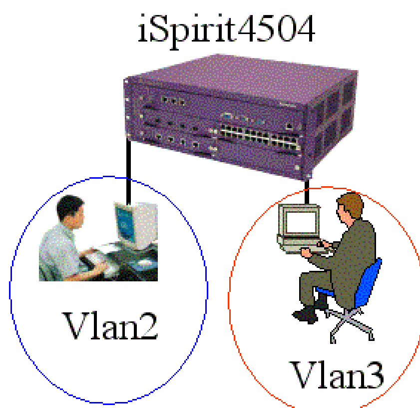
(Version 1.0)

联想网络售后技术支持处

2005 年 5 月

目录

一．基于 PORT（端口）的 VLAN 配置



1．网络需求

4 台计算机分别插 iSpirit 4504 的 4－GT 模块或者 24TX 模块的 1， 2， 3，4 端口，其中 1 和 3 在 VLAN2 内， 2 和 4 在一个 VLAN3 内。要求 VLAN2 中的成员能够相互访问，VLAN3 中的成员能够相互访问，VLAN2 和 VLAN3 成员之间不能相互访问。

端口 VLAN 属性

VLAN	VLAN ID	包含端口
Vlan 2	2	1、3 端口
Vlan 3	3	2、4 端口

2．配置步骤

2.1 使用 4504－4GT 模块（本案例中将此模块安装在第一个插槽上）

4504－4GT 模块可以安装的第一或者二、三插槽上

```
Switch# vlan 2       // 创建 vlan 2
 Vlan 2 added
Switch(vlan-2)#exit
Switch# vlan 3      // 创建 vlan 3
```

Vlan 3 added

Switch(vlan-3)# vlan 2　// 在创建 vlan 2 之后，就可在配置模式下 输入 vlan 2 ，进入 vlan 2 的配置模式

Switch(vlan-2)# untag 1/1 1/3

// 将端口 1/1 和 1/3 加入 vlan 2，如果还有其它端口要加入 vlan 2，那么在 vlan 2 模式下，untag x （x 为其它端口号）；1/1 表示第一槽的第一个端口；1/3 表示第一个槽的第三个端口

Switch(vlan-2)# vlan 3　//进入 vlan 3 配置模式

Switch(vlan-3)# untag 1/2 1/4　//将端口 1/2 和 1/4 加入 vlan 3，如果还有其它端口要加入 vlan 3，那么在 vlan 3 模式下，untag x （x 为其它端口号）

2.2 使用 4504－24T 模块（本案例中将此模块安装在第二个插槽上）

4504－24TX 模块可以安装的第一或者二、三插槽上

Switch# slot 2　//进入 24 口模块的模式（本案例中 24 口模块安装在第二个插槽上，所以在 slot 后面的参数要使用 2，如果安装在第三个插槽上，那么必须输入 3）

Switch(slot-2)# config　//输入 config 进入 24 口模块的配置模式

Slot 2 >

Slot 2 > enable　//输入 enable 进入 24 口模块的特权配置模式

password:　//默认情况下没有密码，直接回车就可以

Slot 2 #　//表示已经进入特权模式

Slot 2 # vlan 2　//创建 vlan2

Vlan 2 added

Slot 2 (vlan-2)# un 1 3　//将 24 口模块上的第 1，3 端口加到 vlan2，配置 24 模块与配置其它模块有点不同，这里直接写上端口号就可以，不像 4GT 模块那样要标明插槽号。

Slot 2 (vlan-2)# vlan 3　//创建 vlan3

Vlan 3 added

Slot 2 (vlan-3)# un 2 4　//将 24 口模块上的第 2，4 端口加到 vlan3。

注：如果同时使用 4 端口模块和 24 端口模块，且每个模块都有 vlan 的配置，假如 4 端口

模块（插在第一插槽）的第 1，3 端口为 vlan2，第 2,4 端口为 vlan3；24 口模块（插在第二插槽）上的第 1,3 端口为 vlan2，第 2,4 端口为 vlan3，使用不同模块上的相同 vlan 都能相互通信，不同 vlan 不能互通，那么配置步骤就是上面提到的两种模块配置方法的结合。

3.排错

如果配置后，发现不同 VLAN 之间的 PC 机不能通信，那是正常现象，因为不同 VLAN 之间要进行通信，必须要经过三层的路由转发。

如果同一 VLAN 内的 PC 机不能进行通信，须作以下验证：

3.1 针对 4GT 模块的排错方法（也适合其它 4 口模块）

1）查看整体有哪些 VLAN

```
Switch# show vlan

-----------------------------------------------
|VID |Name                           | Status |
|----+-------------------------------+--------|
|1   |Default VLAN 1                 | Static |
|---------------------------------------------|
|2   |vlan2                          | Static |
|---------------------------------------------|
|3   |vlan3                          | Static |
|---------------------------------------------|
// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，那么就要重新设置。
```

2）看设置的端口是否在相应的 VLAN 内，并且是以“U”的形势标识的

```
Switch# show  vlan 2   //查看 vlan 2 的配置

Vlan 2 Port Map
```

```
(-=None, M=Tagged, U=Untagged)
|--------------------------------------------------------|
| module |       1        |        2       |       3       |
|--------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|   port | U | - | U | - | - | - | - | - | - | - | - | - |
|--------------------------------------------------------|
```

// 查看 vlan 2 ，发现端口 1/1 和 1/3 标记为 “U”，说明配置正确。 如果 U 不是标记在第一槽位上的第一和第三端口处，那么就是配置有问题，要重新配置。

```
Switch# show vlan 3

Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
|--------------------------------------------------------|
| module |       1        |        2       |       3       |
|--------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|   port | - | U | - | U | - | - | - | - | - | - | - | - |
|--------------------------------------------------------|
```

// 查看 vlan 3 ，发现端口 1/2 和 1/4 标记为 “U”，说明配置正确。如果 U 不是标记在第一槽位上的第二和第四端口处，那么就是配置有问题，要重新配置。

3.2 针对 24 口模块的排错方法

1） 查看整体有哪些 VLAN

Switch# slot 2 //进入 24 口模块的模式（本案例中 24 口模块安装在第二个插槽上，所以在 slot 后面的参数要使用 2，如果安装在第三个插槽上，那么必须输入 3）

Switch(slot-2)# config //输入 config 进入 24 口模块的配置模式

Slot 2 >

Slot 2 > enable //输入 enable 进入 24 口模块的特权配置模式

password: //默认情况下没有密码，直接回车就可以

```
Slot 2 #          //表示已经进入特权模式
Slot 2 # show vlan   //输入查看 vlan 的命令

-----------------------------------------------
|VID |Name                             | Status |
|----+---------------------------------+--------|
|1   |Default VLAN 1                   | Static |
|----+---------------------------------+--------|
|2   | vlan2                           | Static |
|----+---------------------------------+--------|
|3   | vlan3                           | Static |
|----+---------------------------------+--------|

// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，那么就要重新设置。
```

2）查看设置的端口是否在相应的 VLAN 内，并且是以“U”的形势标识的

```
Slot 2 # show vlan 2
Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
-----------------------------------------------------------------
|   Port Number   |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|
|                 |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |U|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-----------------------------------------------------------------
```

// 查看 vlan 2 ，发现端口 1 和 3 标记为 “U”，说明配置正确。 如果 U 不是标记在第一和第三端口处，那么就是配置有问题，要重新配置。

```
Slot 2 # show vlan 3

Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
```

```
-----------------------------------------------------------------
|  Port Number   |0|0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|
|                |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-----------------------------------------------------------------
```

// 查看 vlan 3 ，发现端口 2 和 4 标记为 “ U ”，说明配置正确。 如果 U 不是标记在第二和第四端口处，那么就是配置有问题，要重新配置。

如果出现 vlan 配置和端口所属 vlan 有误，可以在相应的配置模式下前面加 no 。

例如：错误的将 1/4 设置在 vlan2 里，那么可以通过如下命令将其删除。

Switch(vlan-2)# no un 1/4

如果要删除 vlan 2，则可以使用命令 Switch#no vlan 2

二. 基于 802.1Q 的 vlan 配置

1.网络需求

用户	所属 VLAN	连接端口	所属交换机	级连端口
用户 1	vlan2	2	交换机 1	4
用户 2	vlan3	3	交换机 1	4
用户 3	Vlan2	2	交换机 2	4
用户 4	Vlan3	3	交换机 2	4

2. 配置步骤

2.1 使用 4 端口模块（本例中 4 端口模块安装在第一个插槽上）

交换机 1 的配置：

Switch# vlan 2 //创建 vlan 2

Switch(vlan-2)# untagged 1/2 //将端口 1/2 加入 vlan2，同时将端口设置为 untagged 型

Switch(vlan-2)# tagged 1/4 //将端口 1/4 设置为 tagged 型

Switch(vlan-2)# vlan 3 //创建 vlan 3

Vlan 3 added

Switch(vlan-3)# untagged 1/3 //将端口 1/3 加入 vlan3，同时将端口设置为 untagged 型

Switch(vlan-3)# tagged 1/4 //将端口 1/4 设置为 tagged 型

Switch(vlan-3)# exit //退出配置

交换机 2 的配置： 同交换机 1 的配置一样。

2.2 使用 24 端口模块（本例中 24 端口模块安装在第二个插槽上）

交换机 1 的配置：

Switch# slot 2 //进入 24 口模块的模式（本案例中 24 口模块安装在第二个插槽上，所以在 slot 后面的参数要使用 2，如果安装在第三个插槽上，那么必须输入 3）

Switch(slot-2)# config //输入 config 进入 24 口模块的配置模式

Slot 2 >

Slot 2 > enable //输入 enable 进入 24 口模块的特权配置模式

password: //默认情况下没有密码，直接回车就可以

```
Slot 2 #          //表示已经进入特权模式

Slot 2 # vlan 2    //创建 vlan2
 Vlan 2 added
Slot 2 (vlan-2)# un 2   //将端口 2 加入 vlan2，同时将端口 2 设置为 untagged 型
Slot 2 (vlan-2)# ta 4   //将端口 4 设置为 tagged 型

Slot 2 (vlan-2)# vlan 3   //创建 vlan2
 Vlan 3 added
Slot 2 (vlan-3)# un 3    //将端口 2 加入 vlan2，同时将端口 2 设置为 untagged 型
Slot 2 (vlan-3)# ta 4     //将端口 4 设置为 tagged 型
```

交换机 2 的配置：同交换机 1 的配置一样。

3.排错

跨交换机的vlan，在同一个vlan 内的pc 机都能够通信的，如果不能相同，须查看如下：

① 连接pc 机的端口是以“ u ”模式加入这个vlan的。

② 级联端口（本例中是端口4） 是否已经加入到每一个vlan中的，并且在每一个vlan 内都是以“ M ”模式加入的。

3.1 针对4端口模块的排错

查看交换机1 的配置

```
Switch# show vlan
-----------------------------------------------
|VID |Name                             | Status |
|----+---------------------------------+--------|
|1   |Default VLAN 1                   | Static |
|----+---------------------------------+--------|
|2   | vlan2                           | Static |
|----+---------------------------------+--------|
|3   | vlan3                           | Static |
```

```
|----+--------------------------------+--------|

Switch# show vlan 2
Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
|---------------------------------------------------------|
| module |       1         |       2        |       3        |
|--------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|   port | - | U | - | M | - | - | M | M | - | - | - | - |
|---------------------------------------------------------|
```

//端口 1/2 标识为 U，1/4 标识为 M；由于在第二个插槽上安装了 24 端口模块，所以在 2/3 和 2/4 处标识为 M。

```
Switch# show vlan 3

Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
|---------------------------------------------------------|
| module |       1         |       2        |       3        |
|--------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|   port | - | - | U | M | - | - | M | M | - | - | - | - |
|---------------------------------------------------------|
```

//端口 1/3 标识为 U，1/4 标识为 M；由于在第二个插槽上安装了 24 端口模块，所以在 2/3 和 2/4 处标识为 M。

如果查到的结果与实际不符合，请参阅基于端口 vlan 配置实例的排错方法进行排错。
、

查看交换机 2 的配置

由于在本案例中，交换机 2 的配置和 交换机 1 的配置是一样的，所以查看配置方法和结果应该是一样的。如果不一样，请重新配置一下。

3.2 针对 24 端口模块的排错

2） 查看整体有哪些 VLAN

```
Switch# slot 2  //进入 24 口模块的模式（本案例中 24 口模块安装在第二个插槽上，所以在 slot 后面的参数要使用 2，如果安装在第三个插槽上，那么必须输入 3）
Switch(slot-2)# config  //输入 config 进入 24 口模块的配置模式
Slot 2 >
Slot 2 > enable  //输入 enable 进入 24 口模块的特权配置模式
 password:       //默认情况下没有密码，直接回车就可以
Slot 2 #         //表示已经进入特权模式
Slot 2 # show vlan  //输入查看 vlan 的命令

-----------------------------------------------
|VID |Name                             | Status |
|----+--------------------------------+--------|
|1   |Default VLAN 1                   | Static |
|----+--------------------------------+--------|
|2   | vlan2                           | Static |
|----+--------------------------------+--------|
|3   | vlan3                           | Static |
|----+--------------------------------+--------|
```

// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，那么就要重新设置。

2）查看设置的端口是否在相应的 VLAN 内，并且是以“U”的形势标识的

```
Slot 2 # show vlan 2

Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
-----------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|
```

```
|--------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|M|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-----------------------------------------------------------------
```

// 查看 vlan 2 ，发现端口 2 标标识为 “ U ”，端口 4 标识为 “ M ”，说明配置正确。 否则，那么就是配置有问题，要重新配置。

```
Slot 2 # show vlan 3

Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
-----------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|
|--------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|M|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-----------------------------------------------------------------
```

// 查看 vlan 3 ，发现端口 3 标识为 “ U ”，端口 4 标识为 “ M ”，说明配置正确。 否则，那么就是配置有问题，要重新配置。

三．Vlan 间相互通信

1.网络需求

某公司采用 iSpirit4504 构建局域网。为了使公司的局域网达到一个较好的效果，在 iSpirit 4504 上划分两个 vlan，并启用三层转发，实现 vlan 间通信。

本案例中使用了一块 4GT 模块(安装在第二个插槽)和一块 24TX 模块 (安装在第三个插槽)。

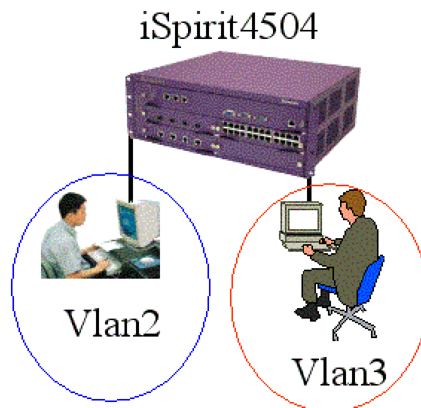
具体要求如下：

vlan 2（4GT 端口 2/1，2/2，24TX 端口 1，2）、vlan 3（4GT 端口 2/3，2/4，24TX 端口 3，4）

vlan 2 的子网接口为 172.20.1.1　子网掩码：255.255.255.0

vlan 3 的子网接口为 192.168.1.1　子网掩码：255.255.255.0

拓扑图如下：



2．配置步骤

2.1 配置 4 端口模块：

1)创建 vlan

```
Switch# vlan 2        // 创建 vlan 2
 Vlan 2 added
Switch(vlan-2)#exit
Switch# vlan 3       // 创建 vlan 3
 Vlan 3 added
Switch(vlan-3)# vlan 2    // 在创建 vlan 2 之后，就可在配置模式下 输入 vlan 2 ，
进入 vlan 2 的配置模式
 Switch(vlan-2)# untag 2/1 2/2    // 将端口 2/1 和 2/2 加入 vlan 2
Switch(vlan-2)# vlan 3    //进入 vlan 3 配置模式
Switch(vlan-3)# untag 2/3 3/4   //将端口 2/3 和 2/4 加入 vlan 3
```

2)查看整体有哪些 VLAN

```
Switch# show vlan

-----------------------------------------------
|VID |Name                          | Status |
|----+-------------------------------+--------|
|1   |Default VLAN 1                | Static |
|-----------------------------------------------|
|2   |vlan2                         | Static |
|-----------------------------------------------|
|3   |vlan3                         | Static |
|-----------------------------------------------|
```

// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，那么就要重新设置。

3）查看设置的端口是否在相应的 VLAN 内，并且是以“U”的形势标识的

```
Switch# show  vlan 2  //查看 vlan 2 的配置

Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
|---------------------------------------------------------|
| module |       1        |       2       |       3       |
|--------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|   port | - | - | - | - | U | U | - | - | - | - | M | M |
|---------------------------------------------------------|
```

// 查看 vlan 2 ，发现端口 2/1 和 2/2 标记为 “U”，说明配置正确。 如果 U 不是标记在第二槽位上的第一和第二端口处，那么就是配置有问题，要重新配置。

```
Switch# show vlan 3
Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
|---------------------------------------------------------|
| module |       1        |       2       |       3       |
```

```
|--------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|   port | - | - | - | - | - | - | U | U | - | - | M | M |
|---------------------------------------------------------|
```

// 查看 vlan 3 ，发现端口 2/3 和 2/4 标记为 “U”，说明配置正确。如果 U 不是标记在第二槽位上的第三和第四端口处，那么就是配置有问题，要重新配置。

2.2 配置 24 端口模块：

1）创建 vlan

Switch# slot 3 //进入 24 口模块的模式（本案例中 24 口模块安装在第三个插槽上，所以在 slot 后面的参数要使用 3）

Switch(slot-3)# config //输入 config 进入 24 口模块的配置模式

Slot 3 >

Slot 3 > enable //输入 enable 进入 24 口模块的特权配置模式

password: //默认情况下没有密码，直接回车就可以

Slot 3 # //表示已经进入特权模式

Slot 3 # vlan 2 //创建 vlan2

Vlan 2 added

Slot 3 (vlan-2)# un 1 2 //将 24 口模块上的第 1，2 端口加到 vlan2，配置 24 模块与配置其它模块有点不同，这里直接写上端口号就可以，不像 4GT 模块那样要标明插槽号。

Slot 3 (vlan-2)# vlan 3 //创建 vlan3

Vlan 3 added

Slot 3 (vlan-3)# un 2 4 //将 24 口模块上的第 2，4 端口加到 vlan3。

2）查看整体有哪些 VLAN

```
Slot 3 (vlan-3)# exit
Slot 3 #
Slot 3 # show vlan
-----------------------------------------------
|VID |Name                            | Status |
|----+--------------------------------+--------|
|1   |Default VLAN 1                  | Static |
```

```
|----+-------------------------------+--------|
|2   | vlan2                         | Static |
|----+-------------------------------+--------|
|3   | vlan3                         | Static |
|----+-------------------------------+--------|
```

// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，那么就要重新设置。

3）查看设置的端口是否在相应的 VLAN 内，并且是以“U”的形势标识的

```
Slot 3 # show vlan 2
Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
-----------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |U|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-----------------------------------------------------------------
```

// 查看 vlan 2 ，发现端口 1 和 2 标记为 “U”，说明配置正确。 如果 U 不是标记在第一和第二端口处，那么就是配置有问题，要重新配置。

```
Slot 3 # show vlan 3

Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
-----------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
-----------------------------------------------------------------
```

// 查看 vlan 3 ，发现端口 3 和 4 标记为 “U”，说明配置正确。 如果 U 不是标记在第三

和第四端口处，那么就是配置有问题，要重新配置。

如果出现 vlan 配置和端口所属 vlan 有误，可以在相应的配置模式下前面加 no 。

例如：错误的将 1/4 设置在 vlan2 里，那么可以通过如下命令将其删除。

Switch(vlan-2)# no un 1/4

如果要删除 vlan 2，则可以使用命令 Switch#no vlan 2

2.3 设置子网 ip

配置完 vlan 之后，就可以配置子网 ip，即给每个 vlan 配上一个 ip 地址，使得启用三层转发功能。

1） 配置 vlan2 和 vlan3 的子网 ip

```
Switch# int vlan 2
Switch(interface-vlan2)# ip add 172.20.1.1 255.255.255.0
Switch(interface-vlan2)# int vlan 3
Switch(interface-vlan3)# ip add 192.168.1.1 255.255.255.0
Switch(interface-vlan3)#exit
```

2） 查看配置结果

```
Switch# show int vlan 2

****************************************************
 vlan 2 interface
 IP address:      172.20.1.1
 netMask:         255.255.255.0
 Status:          Active
****************************************************

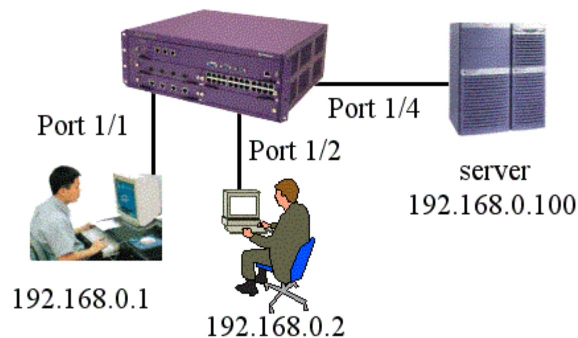
Switch# show int vlan 3
```

```
****************************************************
 vlan 3 interface
 IP address:      192.168.1.1
 netMask:         255.255.255.0
 Status:          Active
****************************************************
```

四．私有 vlan 配置

1．网络需求

3 台计算机分别连在交换机 iSpirit 4504 的 1， 2， 4 端口，其中连接 4 端口的计算机作为服务器。PC1 和 PC2 均可以访问 4 口的服务器，但是 PC1 和 PC2 之间不能互相访问。网络拓扑图如下：



2.配置步骤

2.1 以 4 端口模块为配置实例

Switch# private 1　　　　　　　　　　　　　　　// 创建私有 vlan 组 1

//注意：

iSpirit 4504 最多支持 12 组私有 vlan，私有 vlan 组号的范围 1~ 12。

Switch(privatevlan-1)# vlan 2 4 2　//配置私有vlan包涵的vlan范围

Switch(privatevlan-1)# isolate 1/1 1/2 //配置隔离端口

Switch(privatevlan-1)# promiscuous 1/4 //配置混杂端口

Switch(privatevlan-1)# enable //启用私有vlan

Switch# show pri 1 //查看私有vlan 1 的配置信息

Private vlan group : 1

status : active

//这里的active是命令 " enable " 所起的作用，如：witch(privatevlan-1)# enable

max vlan number : 4

min vlan number : 2

primary vlan number : 2

promiscuit port : 1/4

iSolatePort port : 1/1 1/2

2.2 以24端口模块为配置实例（假设24口模块安装在第二个插槽上）

Switch# slot 2 //进入 24 口模块的模式（本案例中 24 口模块安装在第二个插槽上，所以在 slot 后面的参数要使用 2，如果安装在第三个插槽上，那么必须输入 3）

Switch(slot-2)# config //输入 config 进入 24 口模块的配置模式

Slot 2 >

Slot 2 > enable //输入 enable 进入 24 口模块的特权配置模式

password: //默认情况下没有密码，直接回车就可以

Slot 2 # //表示已经进入24模块的特权配置模式

接着的配置与4口模块的配置一样。

24模块上的私有vlan和4口模块上的私有vlan是相对独立的。

// 注意：

这里为什么要设置为vlan 2 4 2 ，即 2（最小数） 4（最大数） 2 （私有vlan 1中的主vlan号）？这是因为在本案例中，我们要设置2个隔离端口，0个共用体，所以需要使最大数减去最小数等于或者大于2 ***（如果是2个隔离端口和1个共用体，那么就要大于等于3）*** *。这里的最小数2，并不一定要用2，也可以用其它数。只要保证最大数减去最小数等于或者大于4。主vlan号，就是要包含在最大数和最小之间的任一个，一般都是选择最小那个，在本案例中，我们选择了2。*

如果配置了私有vlan之后，还要设置普通的vlan，例如：基于端口或者基于802.1Q的vlan。那么这些vlan的vlan号是不能和私有vlan中的vlan号重叠。例如：本例中，私有vlan中的vlan号包含了2～4，所以创建其它普通vlan时就不能用到这些vlan号。

在设置私有vlan时，也可以设置共用体组，（在一个私有vlan里，最多可以支持6个共用体组），同一共用体组里的端口是可以相互访问，也可以与混杂端口相互访问，但不能与不同的共用体组相互访问，也不能与隔离端口相互访问。有关混杂端口，共用端口，隔离端口三者之间的关系，也即哪种端口可以相互访问，哪种端口不能相互访问，请参阅1.4附件

共用体组的设置命令也是在私有vlan 的配置模式下执行的。例如，在私有vlan 1 下创建共用体组1，此共用体组包含端口1/1 和1/2。注意，这两个端口要设置为某个共用体组内所包含的端口，那么它们就不能被设置为混杂端口，隔离端口。

```
Switch# privatevlan 1
Switch(privatevlan-1)# community 1  1/1 – 2
```

特别注意

在私有vlan里每个端口的模式只能属于混杂，隔离，共用三种模式中的一种

1.3 排错

如果配置不成功可能有以下几个原因：

1) min-vlanid 值比max-vlanid 大。

2) primary-vlanid 不在min-vlanid 到max-vlanid 范围内。

3) max-vlanid 值减min-vlanid 大于12（对于4端口模块）；大于26（对于24TX模块）。
4) min-vlanid 值到max-vlanid 的VLAN范围有至少一个VLAN被普通VLAN占用。
5) 私有VLAN 组与其它的私有VLAN 组有VLAN 范围重叠的现象。
6) 如果该私有VLAN 组处于生效（active）状态，就不能够对该私有vlan 做任何配置
7) 私有VLAN 所包含的vlan 数至少应该大于等于私有vlan 的(私有端口个数+ 公用端口组数+1)
8) 私有VLAN 组内没有混杂端口。
9) 私有VLAN 组内既没有隔离端口又没有共用端口组。
10) 私有VLAN 组内混杂端口、共用端口和隔离端口有重叠的现象。
11) 私有VLAN 组与其它的私有VLAN 组有混杂端口、共用端口和隔离端口重叠的现象。
12) 如果私有VLAN组内的混杂端口、共用端口或隔离端口属于普通VLAN的untagged 成员，则要从该普通VLAN中清除这些端口，是这些端口不属于该普通VLAN的成员

1.4 附件

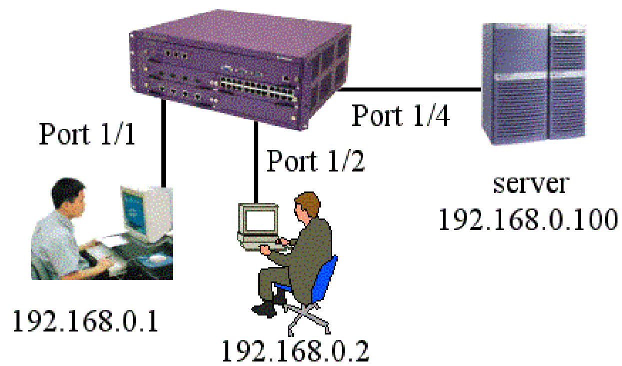
私有 VLAN 端口通信关系

	混杂端口	组 1 共用端口	组 2 共用端口	隔离端口
混杂端口	可以	可以	可以	可以
组 1 共用端口	可以	可以		
组 2 共用端口	可以		可以	
隔离端口	可以			

五．Vlan 内端口隔离配置

1.网络需求

有两个用户在同一个 vlan 内（默认为 vlan1），为了每个用户的相对独立保密的情况下，需要同一个 vlan 内的任意两个用户不能够相互访问(两个用户分别连接在 1/1 和 1/2)，但是用户的端口都需要通过级联端口 1/4 向上访问网络。这种需求可以通过 vlan 内的端口隔离的功能来实现。



2.配置步骤

2.1 以 4 端口模块为配置实例

1）将端口 1 和 2 设置为隔离端口，但可以通过端口 4 进行上联访问。

```
Switch# port 1/1
Switch(port 1/1)# separated 1/4
Switch(port 1/1)# port 1/2
Switch(port 1/2)# separated 1/4
```

2）查看配置信息

```
Switch# show separated
Port                    Egress Port           Status
 1/1                         1/4             Separated
 1/2                         1/4             Separated
 1/3                         N/A             unSeparated
 1/4                         N/A             unSeparated
```

2.2 以 24 端口模块为配置实例

Switch# slot 2 //进入 24 口模块的模式（本案例中 24 口模块安装在第二个插槽上，所以在 slot 后面的参数要使用 2，如果安装在第三个插槽上，那么必须输入 3）

Switch(slot-2)# config //输入 config 进入 24 口模块的配置模式

Slot 2 >

```
Slot 2 > enable   //输入 enable 进入 24 口模块的特权配置模式
 password:        //默认情况下没有密码，直接回车就可以
Slot 2 #          //表示已经进入24模块的特权配置模式
```

接着的配置与4口模块的配置类似。

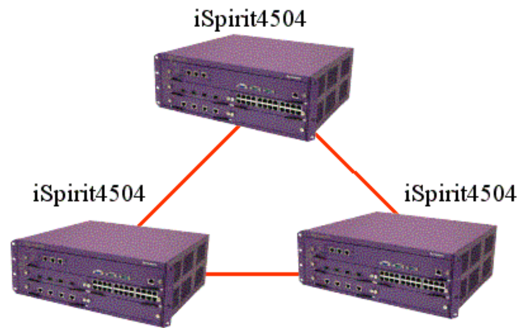
查看配置信息

```
Switch# show separated
Port                  Egress Port              Status
   1                        4                 Separated
   2                        4                 Separated
   3                      N/A                  unSeparated
   4                      N/A                  unSeparated
   5                      N/A                  unSeparated
   6                      N/A                  unSeparated
   7                      N/A                  unSeparated
   8                      N/A                  unSeparated
   9                      N/A                  unSeparated
  10                      N/A                  unSeparated
  11                      N/A                  unSeparated
  12                      N/A                  unSeparated
  13                      N/A                  unSeparated
  14                      N/A                  unSeparated
  15                      N/A                  unSeparated
```

六．STP（生成树）配置

1.网络需求

为了避免三台 iSpirit4504 连接在一起构成环路，需要配置 STP（生成树协议）。



2.配置步骤

1） 在全局模式下启用 stp 协议

Switch# stp　　用 STP，默认情况下交换机在全局上是关闭 STP，在全局模式下输入 stp,则启用 stp。

2）确认生成树协议在每一台交换机上是打开的

Switch# show switch

```
 Ip Address         : 192.168.0.1
 Subnet Mask        : 255.255.255.0
 Default Gateway    : 0.0.0.0
 MAC Address        : 00:09:ca:13:4e:00
 Spanning Tree      : Enable
 IGMP Snooping      : Disable
 DhcpRelay          : Disable
 Rip                : Disable
```

上述的 Spanning Tree 是 Enable，说明 stp 协议已经启用。

如果需要关闭生成树协议的运行，需要输入命令

Switch# no stp

生成树协议的高级命令：

设置其中第一台交换机为根交换机，需要设置他的桥优先级比其他两个桥的优先级要小，默认

优先级为 32768

Switch# stp bridge priority A   stp bridge priority (0=<A<=65535)

在全局模式下启用了 stp ，那么交换机上的所有端口运行 stp，如果要使交换机的某个端口不参与生成树的运行，需要对特定的端口关闭生成树功能.

Switch# disable stp ports portnumber

如果某个端口已经关闭了 stp 的功能后又想把它开启。

那么使用命令 Switch# enable stp ports portnumber

3．排错

1）察看哪一个交换机被选为根网桥：

```
Switch# show stp bridge
--- Designated Root Information ---
 Priority                  : 32768
 MAC Address               : 00:09:ca:13:4e:00
 Hello Time                : 2s
 Forward Delay             : 15s
 Max Age                   : 20s

 --- Bridge STP Information ---
 Bridge Priority           : 32768
 MAC Address               : 00:09:ca:13:4e:00
 Root Path Cost            : 0
 Root Port                 : 0
 Bridge Hello Time         : 2s
 Bridge Forward Delay      : 15s
 Bridge Max Age            : 20s
```

2）察看生成树中交换机的端口状态：

Switch# show stp port 1/1

```
--- Port Information ---
Module/Port              : 1/1
STP Port                 : Enable
Port ID                  : 6
Priority                 : 128
State                    : Disabled
Path Cost                : 4
Designated Cost          : 0

--- Designated Root Information ---
Priority                 : 32768
MAC Address              : 00:09:ca:13:4e:00

--- Designated Port Information ---
Port ID                  : 6
Priority                 : 128

--- Designated Bridge Information ---
Priority                 : 32768
MAC Address              : 00:09:ca:13:4e:00
```

//注意：

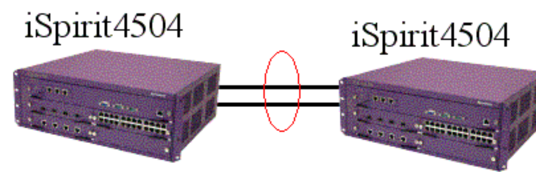
以上用到的几个调式命令例子，所显示的信息并不代表其它交换机在实际运行环境中的信息。在实际应用中，要根据需求分析。

七．Trunk 端口聚合配置

1. 网络需求

为了增加两台 iSpirit4504 连接间的带宽，同时提供冗余功能，保证其中一条链路出了问题时，其它链路都可以正常使用，因此，在这里使用了 trunk 配置。

在交换机 1 和交换机 2 之间做 trunk 链路，各自捆绑 1/1 和 1/2，1/3 端口做链路聚合。



2. 配置步骤

创建一个 trunk 1,其包含插槽 1 的 1/1-3 端口

Switch#trunk config 1 1 1/1-3

以上命令个参数的解析

Switch# trunk config ?

A trunk_Id: (0<=A<=28) //设置 trunk 的 id 号，范围为 0-28

Switch# trunk config 1 ?

A trunk_Rtag: (1<=A<=6) //设置 trunk 的类型，总共有 6 中类型，范围为 1-6

Switch# trunk config 1 1 ?

M/P module/port(1<=p<=4)(1<=m<=3)

M/p1-p2 Module/portmin-portmax(1<=p1,p2<=4)

//注意:

配置 trunk 时，两边交换机的端口数量要一致，速度、双工等端口参数都要完全一致，但不必两边的端口号一一对应。

上述配置是以 4 端口模块为例子，如果是采用 24 模块，那么就要进入 24 模块的配置模式，其他配置都一样。

3. Trunk 删除命令

删除一个 trunk 组

Switch# no trunk ?

A trunk_Id(0<=A<=28)

4.排错

1）如果 trunk 没有起作用，需要查看以下状态，检查所配置的 trunk 是否激活，包含的端口数量和端口号是否正确。

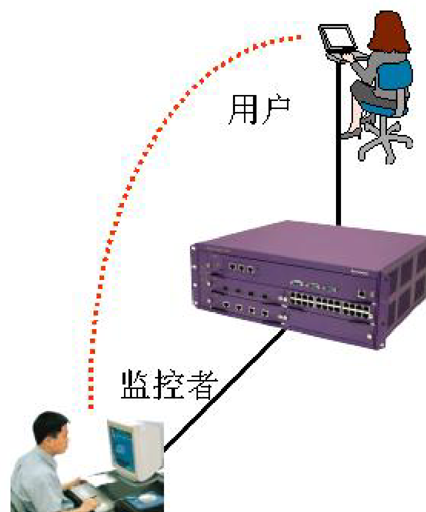
```
Switch# show trunk
TGID        RTAG          status       Ports
 1           1             Active       1/1-1/3
```

2）加入 trunk 组的几个端口一定要属于同一个 vlan，速率，双工等端口属性都要设置一样。

八. Mirror （端口镜像）配置

1.网络需求

在一台交换机中，用户 1 和用户 2 正在通信，正常情况下其他端口的用户是无法获取其通信信息的，为了检测数据流是否正常，监测者需要获取其数据流，就要用到端口镜像问题。用户 1 连接到端口 1，用户 2 连接到端口 2 监测者连接在端口 4，使监测者能够捕捉到其数据流。



2.配置步骤

2.1 以 4 端口模块为配置实例

```
Switch# mirror  port   1/4    //监控者的端口
```

```
Switch# mirror egress  1/1-2    //被监控者出口流量的端口
Switch# mirror ingress  1/1-2  //被监控者入口流量的端口
```

用 show mirror 命令进行确认

```
Switch# show mirror
 Mode        : L2
 mirror Port      : 1/4
 egressPortList  : 1/1-1/2
 ingressPortList : 1/1-1/2
```

2.2 以 24 端口模块为配置实例

```
Slot 1 # mirror
Mirror Port: 4
Egress ports_list: 1-2
Ingress ports_list: 1-2
```

// 注意：24 口模块配置端口 mirror 是采用交互式的命令，这一点与 4 端口模块有点不同。

用 show mirror 命令进行确认

```
Slot 1 # show mirror
Mirror Mode: L2
Mirror Port: 24
Egress ports_list: 1-2
Ingress ports_list: 1-2
```

3.排错

1) 不要把镜像端口和被镜像端口搞反了。

   镜像端口是 mirror ports,指的是观测者所在的端口

   被镜像端口是 Egress ports（外出数据流），Ingress ports （进入数据流），指的是被观测的端口

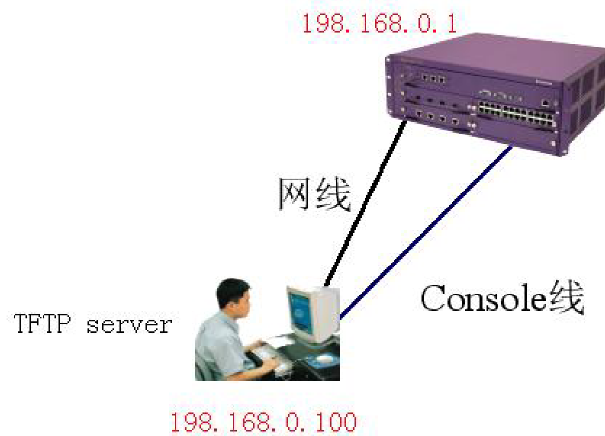
九．Configuration 文件备份

1．网络需求

1） 把交换机的配置文件上传（备份）到 TFTP 服务器上；

2） 把存放到 TFTP 服务器上的配置文件下载到交换机

网络拓扑图如下：



2．配置步骤

网络环境如下

硬件：交换机，计算机，串口线，网线。

软件：windowns 操作系统，TFTP 服务器软件（tftpd32.exe 或者其它 tftp 软件）

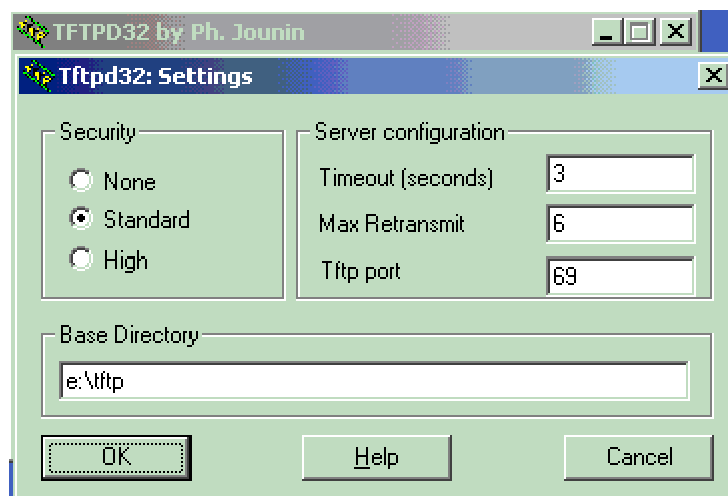
1）设置 TFTP 服务器的 IP 地址为 192.168.0.100，iSpirit 4504 交换机的 IP 地址为 192.168.0.1，并确保 TFTP 和交换机的 IP 之间能够相通

交换机 ip 地址的配置如下：

switch>enable

switch#ip add 192.168.0.1 255.255.255.0 //默认情况下，交换机是已经配置好 ip 地址，请根据实际环境作调整。

2）设置 pc 机的 ip 地址为 192.168.0.100 ，并运行 tftp 软件。



上述 e:\tftp 为下载配置文件所在的位置（即配置文件存放在 e:\tftp 目录下），可以根据实际情况进行设置。

3）把交换机的配置文件上传（备份）到 TFTP 服务器上,具体操作如下，在交换机上执行

Switch# upload configuration 192.168.0.100 文件名

 uploading configuration ......

4）如果为了方便，不想重新配置交换机，那么可以把保存在 TFTP 服务器上的配置文件向下传到交换机上，具体操作如下，在交换机上执行

Switch# download configuration 192.168.0.100 文件名

 Do you wish to continue? [Y/N]: y

//注意：以上的操作方法适合主控模块配置文件的下载和上传（默认情况下，主控上的默认管理地址为 192.168.0.1）。如果是要下载或者上传 24 端口模块的配置文件，那么先进入 24 端口模块配置模式，接下来的配置步骤都一样（24 端口模块默认情况下也有一个管理地址，而且插在第一插槽时，ip 地址为 192.168.0.2，插在第二插槽时，ip 地址为 192.168.0.3。）

3.排错

如果上传或者下载文件不成功，需要注意以下几个方面：

1） tftp 服务器和交换机之间的 IP 是一定要相互能通。

2） tftp 服务器的 tftp 服务一定要打开。

3） 在交换机上执行的下传或下载配置文件的命令一定要写正确，特别是配置文件的名字一定

要正确，区分大小写。

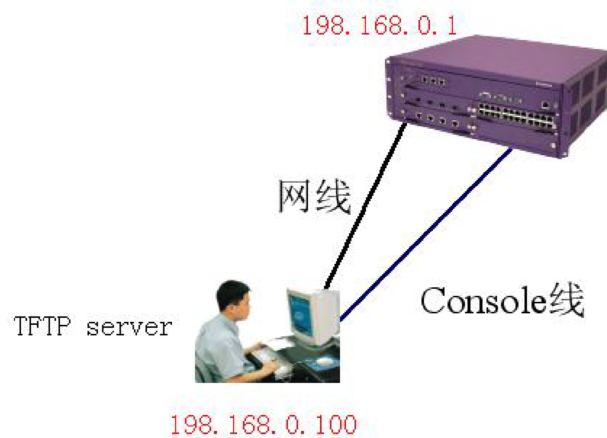
准备好的配置文件一定要放置到 tftp 服务器指定的目录下。

十．IMAGE 软件升级

1．网络环境

硬件：交换机，计算机，串口线，网线。

软件：windowns 操作系统，TFTP 服务器软件（tftpd32.exe 或者其它 tftp 软件）



2．配置步骤

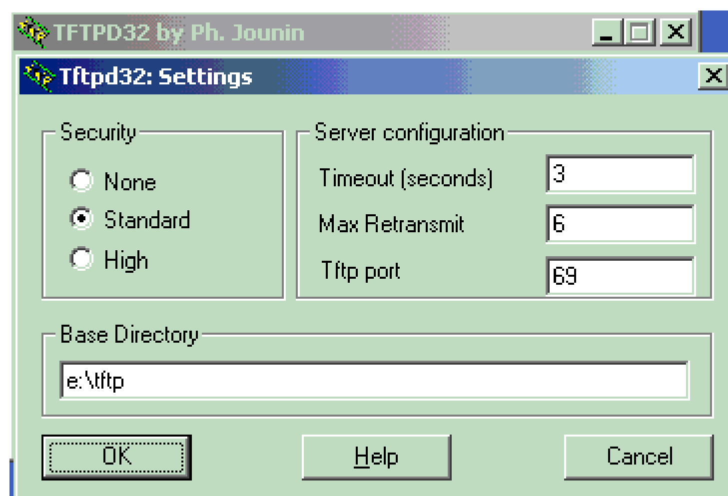
1）配置交换机的 ip 地址

Switch>enable

Switch#ip add 192.168.0.1 255.255.255.0 //默认情况下，交换机是已经配置好 ip 地址，请根据实际环境作调整。

Switch#show switch //可以看到刚才配置的 ip 地址

2）设置 pc 机的 ip 地址为 192.168.0.100 ，并运行 tftp 软件。



上述 e:\tftp 为升级文件所在的位置（即升级文件存放在 e:\tftp 目录下），可以根据实际情况进行设置。

3）在超级终端下，输入 download 命令，开始下载镜像文件。

```
Switch# download image 192.168.0.100 iSpirit30261V12.img
 Do you wish to continue? [Y/N]: y
 Don't Shut down power until completed!
 downloading image ......
```

一直等到交换机提示升级完成，然后才能重新启动交换机

//注意：

以上的升级方法适合主控模块的一般升级（默认情况下，主控上的默认管理地址为 192.168.0.1）。如果是要升级 24 端口模块，那么先进入 24 端口模块配置模式，接下来的配置步骤都一样（24 端口模块默认情况下也有一个管理地址，而且插在第一插槽时，ip 地址为 192.168.0.2，插在第二插槽时，ip 地址为 192.168.0.3。）

如果要升级 bootrom，那么具体操作步骤请见《iSpirit4504bootrom 升级指南》。

在升级交换机的过程中，不能断电。如果中途断电，很可能造成交换机损坏。

3．排错

交换机映像文件升级不成功，需要查找以下几个原因：

1） 交换机和 TFTP 服务器之间是否 IP 能够通信。

2） TFTP 服务器是否正常启动，并且启动所用的 IP 地址就是交换机所能够 PING 通的。

3） 映像文件是否放到了 TFTP 服务器所指定的特定位置。

4） 在交换机上执行升级映像文件时，映像文件的名字一定不要写错。

十一．snmp 配置

1.网络需求

有一个 SNMP 管理站上面运行 SNMP 管理软件，管理站的 IP 地址为 192.168.0.100。现在，管理站要管理其中一台 IP 地址为 192.168.0.1 的交换机。由于该工作站有两个管理者，一个管理者只有对交换机有查看信息的权限，另一个管理者可以对交换机进行设置。因此。在交换机上打开 SNMP 后（默认是打开的），配置了 snmp 的 community ，一个为只读，另外一个为读写。其中，只读的 community 设置为 public，读写的 community 设置为 private。



3.配置步骤

1） 默认情况下，iSpirit4504 交换机已经启动了 snmp ，所以设置 snmp 时，只要设置 snmp community 和相关参数就可以。

//默认情况下，已经有 public 这个 community。

```
Switch# snmp community
Community Name : public
```

//设置 community 为 public，这个参数是一个字符串，内容不限

View Name(internet) :

 ReadOnly(1),ReadWrite(2)

Permission : 1   //选择 1，将属性设置为只读

Switch# snmp community

Community Name : private

//设置 community 为 private，这个参数是一个字符串，内容不限

View Name(internet) :

 ReadOnly(1),ReadWrite(2)

Permission : 2   //选择 2，将属性设置为为读写。

查看 snmp community 的配置

Switch# show snmp community

CommunityName	ViewName	Permission	Status
public	internet	ReadOnly	Active
private	internet	ReadWrite	Active

如果查看到上述的配置信息。一般就没有问题了。接着就是对管理站进行相关设置。管理站的设置，请查阅管理软件的相关配置手册。

2）配置了 snmp 之后，还可以进行可选配置，如 trap

trap 指的是当交换机发生特殊情况时，主动向 snmp 管理站发送 snmp 信息。

需要配置 trap 功能，选择 snmp 版本为 2

Switch# snmp trap

trap name : test

Target Ip Addr: 192.168.0.100

 snmpv1(1),snmpv2(2),snmpv3(3)

Version : 2

查看配置信息：

```
Switch# show snmp trap
- Trap Name        : test
 Transport Domain : 1.3.6.1.6.1.1
 Target ip        : 192.168.0.100
 Target port      : 162
 TimeOut          : 1500
 Retry Count      : 0
 Version          : snmp V2
 Storage Type     : nonvolatile
 Status           : Active
```

3.排错

如果 snmp 不起作用，需要查看以下几个方面：

1） 交换机上需要配置读写或只读的 community ,例如只读为 pubic ,读写为 private，这两个字符串要与管理站上的管理软件设置一致。
2） 同上述类似的问题，也需要在 snmp 服务器上配置同样的 community，才能够使 snmp 服务器对交换机进行远程察看或者管理。
3） 交换上上是否关闭了 snmp。(默认情况是打开 snmp 功能)。可以通过 show manager 查看 snmp 是否打开。关闭 snmp 的命令为： disable snmp；打开则为 enable snmp

如果交换机不能主动发起 trap 信息给 snmp 服务器，需要查看以下：

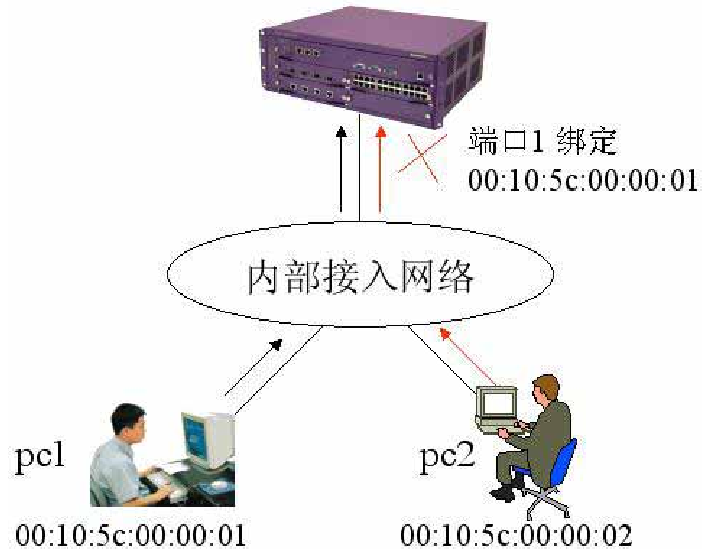
1） 需要在交换机上设置 trap 接收者的 ip 地址，也就是 snmp 服务器的 ip 地址。

确保交换机的 ip 地址和 snmp 服务器之间的 ip 是能够相通的。

十二．MAC 绑定配置

1．网络需求

某公司想通过 mac 地址来控制接入 iSpirit4504 交换机的用户，只允许 mac 为 00:10:5c:00:00:01 可以通过端口 1 接入网络。拓扑图如下：



3．配置步骤

3.1 以 4 端口模块为配置实例：

1） 将 mac 绑定到端口 1

Switch# mac bind 1/1 1 00:10:5c:00:00:01 // 1/1 为端口号，接下来的 1 为 vlan 号

2） 查看 mac 绑定信息

Switch# show mac bind

Module/port	VLAN	macAddress	STATUS
1/1	1	00:10:5c:00:00:01	Active

3.2 以 24 端口模块为配置实例：

1)进入 24 端口模块配置模式

2)接下的配置步骤与 4 端口配置类似

//注意：

*当 mac 地址为 00:10:5c:00:00:01 绑定在端口 1，那么就不能将此 mac 地址绑定到其它端口（在本例中，所有端口都是在 vlan1 里）。**如果 iSpirit4504 划分了多个 vlan，那么同一个 mac 地址可以绑定到不同 vlan 里的端口。**在上述的实例中,端口 1 绑定了 00:10:5c:00:00:01，那么端口 1 就只能允许 mac 地址为 00:10:5c:00:00:01 通过该端口，而且 mac 地址 00:10:5c:00:00:01 是不能通过其它端口进入网络的。ISpirit4504 一个端口最多可以绑定 128 个 mac 地址。*

Mac 地址的绑定方法除了上述的手工绑定之外，还有一种叫自动 mac 绑定。这种使用方法是当交换机学习到 mac 地址之后，使用命令：mac bind 端口号 进行自动绑定。如果端口还没有学习到 mac，那么使用 mac bind 是绑定不到 mac 地址的。采用动态 mac 绑定方法，一个端口最多也是只能绑定 128mac 地址，但每个端口学习到 mac 地址多于 128 个时，那么每个端口只有前 128mac 地址可以在自动绑定方法中被绑定。自动 mac 绑定是在端口没有进行手工 mac 绑定的情况下才可以进行绑定，但是，手工 mac 绑定则不管端口是否进行了自动绑定，也就端口进行了自动绑定之后，还是可以进行手工 mac 绑定,只要绑定的 mac 地址数不要超过 128 个就可以。

4. 排错

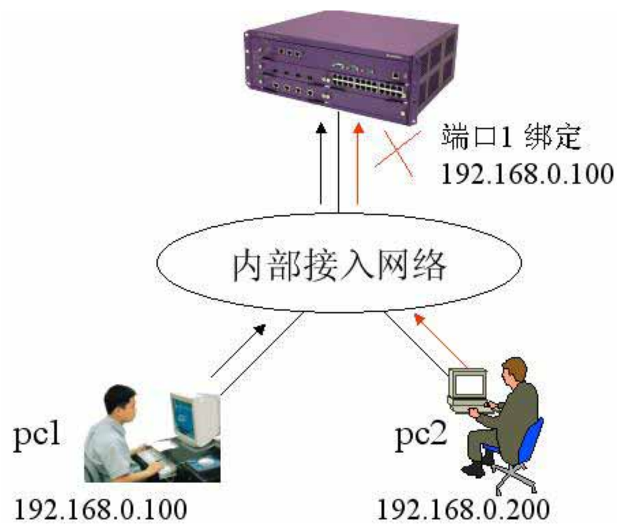
1）进行 mac 绑定时，如果绑定不成功，那么要检查一下 mac 地址是否正确，是否绑定在正确的端口上。

2）进行 mac 绑定，要注意 mac 绑定的规则。简单的规则可以参照配置步骤的注意事项。如果想了解更详细的信息，可以查阅 iSpirit4504 用户手册。

十三．IP 绑定配置

1.网络需求

某公司想通过 ip 地址来控制接入 iSpirit4504 交换机的用户，只允许 ip 地址为 192.168.0.100 的用户可以通过端口 1 接入网络。拓扑图如下：



2.配置步骤

1) 将 ip 地址为 192.168.0.100 绑定到端口 1

Switch# ip bind 1/1 192.168.0.100 //“1/1”为端口号，这里与 mac 绑定有点不同，没有涉及到 vlan 号

2) 查看端口 1 的 ip 绑定信息

```
show ip bind 1
module/port          ipAddress        macAddress
  1/1              192.168.0.100     00:00:00:00:00:00
```

如果是采用 24 端口模块，那么就要先进入 24 端口模块的配置模式，接下来的配置与 4 端口模块类似。

//注意：

通过以上的配置，可以对端口 1/1 和 ip 地址为 192.168.0.100 进行控制。端口 1/1 只能接 ip 地址为 192.168.0.100 的用户。

Ip 绑定与 mac 绑定的规则有点不同。交换机的不同端口可以绑定相同的 ip 地址。如果一个端口 A 绑定了一个 ip 地址，另一个端口 B 没有绑定 ip 地址，那么端口 A 所绑定的 ip 地址的用户是可以通过端口 B 访问网络。一个端口最多可以绑定 127 个 ip 地址。

3.排错

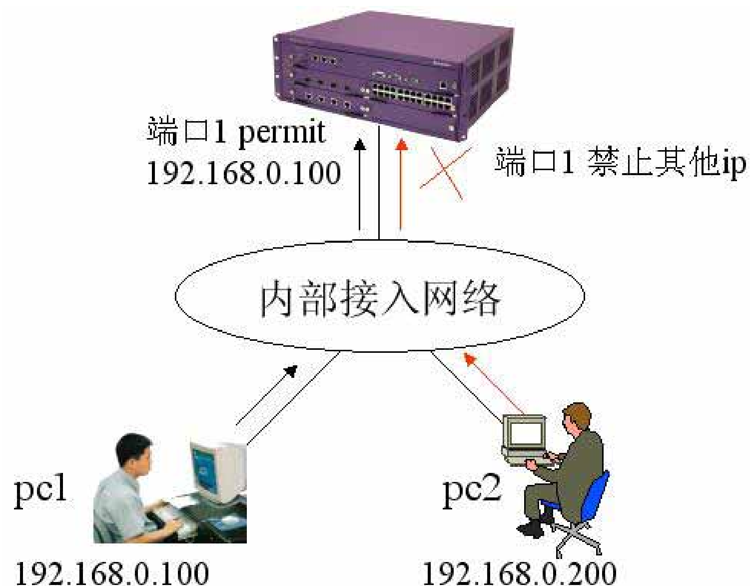
1）进行 ip 绑定时，如果绑定不成功，那么要检查一下 ip 地址是否正确，是否绑定在正确的端口上。

2）进行 ip 绑定，要注意 ip 绑定的规则。简单的规则可以参照配置步骤的注意事项。如果想了解更详细的信息，可以查阅 iSpirit4504 用户手册。

十四．ACL 访问控制列表配置

1.标准 IP 规则的 ACL

1）实例：控制交换机端口 1 只能接上 ip 地址为 192.168.0.100 的 pc。如果是其它 ip 地址的 pc 就不能连接到端口 1。也即 ip 地址为 192.168.0.100 的 pc 发出的数据流可以通过交换机的端口 1 转发，而 ip 地址的 pc 发出的数据流不可以通过交换机的端口 1 转发。



2）配置：

A ：Switch# access-list 1 permit host 192.168.0.100

//默认情况下,在上述列表的规则组 1 之后隐含了一条规则 deny any 的规则,此规则是禁止所有。 一个规则组里可以包含 128 的规则。例如，上述的规则组 1，它除了配置一条规则之外（本例中是 access-list 1 permit host 192.168.0.100 ），还可以配置更多条规则，例如：access-list 1 permit host 192.168.0.123

标准 ip 规则的 acl 的规则组号为 1~199

B:把这标准访问控制列表（access-list 1）应用到 1 端口（对 1 端口流入的数据流做控制）

Switch# port 1/1

Switch(port 1/1)# acl-filter 1

//如果没有将访问控制列表应用到端口上，那么此访问控制列表是不起作用的。

//以上 acl 的配置是以 4 端口的配置模块为例子。如果是使用 24 端口模块，那么就要先进入 24 端口模块的配置模式。由于 24 端口模块比 4 端口模块的端口多了几倍，所以对于多个端口要应用相同的 acl，那么可以一次性对多个端口进行应用。例如，要将访问控制列表 100 应用到端口 10－20 上，那么可以进行如下的简单操作：

slot 2# port 10-20

slot 2(port 10-20)# acl-filter 100

3）排错：

在配置访问控制列表之前确保所有 ip 之间都是通的，然后再添加访问控制列表

这条访问控制列表允许源地址为 192.168.0.100 的 IP 数据流通过交换机。用 show access-list 命令列出访问控制列表进行查看。默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其它都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

Switch# show acl-filter

ACL group and Port Configuration Information

module/port　　　　　　groupId　　　　　　status

1/1　　　　　　　　　　1　　　　　　　　　Active

Switch# show access-list 1

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type

SP - Source Port, DP - Destination Port, PT - Protocol Type

SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

Standard IP access list:

GroupId 1 :   reference count(1)

R 1   permit SI 192.168.0.100 Active

//注意：标准的 acl 不仅仅是上述提到的 host 方式，还有其他两种方式。可以通过帮助命令看到。例如：(以下的例子为标准 acl permit 下的几种模式)

Switch# access 1 permit ？ //输入 access 1 permit（或者 deny） 并带上参数“ ？ ”查

看标准 acl 下的几种模式

A.B.C.D　　Source address

//采用网段的方式。例如要控制的网段是 192.168.1.0,那么就可以使用 access 1 permit 192.168.1.0 0.0.0.255

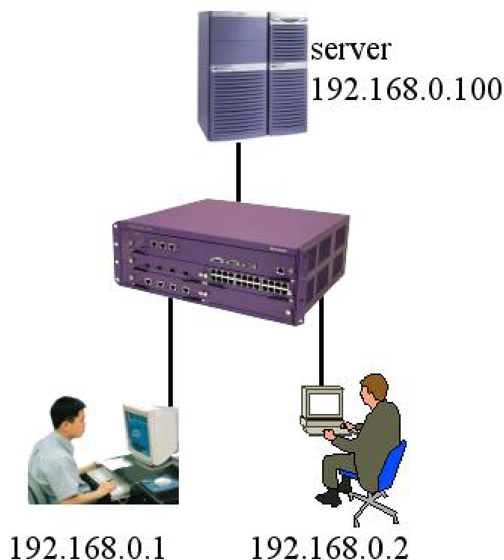
any　　Any host

//采用任何主机方式，则使用参数 any 。例如 access 1 permit any

host　　A single host address

//采用指定某主机方式，则使用参数 host。例如 access 1 permit host 192.168.1.1

2.扩展 IP 规则的 acl（web 控制实例）



1) 网络需求：

在这个网络中，web 服务器的 ip 地址为 192.168.0.100（对应的端口为 4)，用户的 ip 地址为 192.168.0.1~192.168.0.2（对应的端口为 1~2）。为了保护服务器的安全，只允许用户对服务器进行 web 访问。

2) 配置步骤：

A. 建一条只允许用户访问服务器的规则：

```
Switch# access 200 permit tcp 192.168.0.1 0.0.0.255 host 192.168.0.100 www
```

//扩展 ip 规则的规则组号为 200～399

B.把访问控制列表 200 应用到 1～2 端口，对流入的数据流做控制

```
Switch# port 1
Switch(port 1)# acl-filter 200
Switch# port 2
Switch(port 1)# acl-filter 200
```

如果是采用 24 端口模块，那么先进入 24 端口模块的配置模式，其它配置与上述类似。

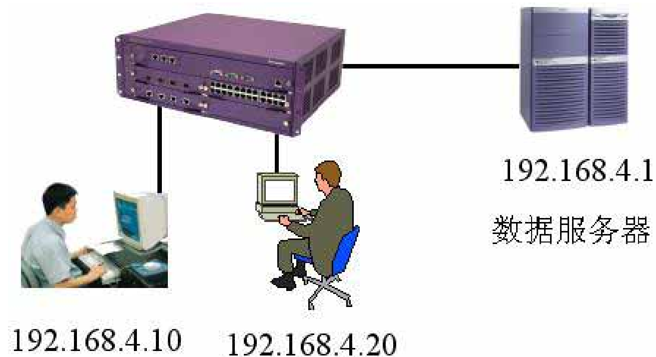
3）排错：

A 对于特定的应用需要指定特定四层网络端口。而且默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

B 需要用 show access-list / access 命令来进行查看访问控制列表配置是否正确

```
Switch# show acl-filter
ACL group and Port Configuration Information
module/port            groupId             status
  1/1                    200                 Active
  1/2                    200                 Active
Switch# show access
 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.
Extended IP access list:
  GroupId 200 : reference count(0)
R 1 permit tcp SI 192.168.0.0 0.0.0.255 DI 192.168.0.100 www Active
```

3.扩展 IP 规则的 acl（单向 ICMP 访问控制实例）



1） 网络环境：

为了防止一般用户刺探网络数据服务器，需要一般用户不能够 PING 通数据服务器，但是数据服务器可以 PING 通其他所有用户。这就需要用到 ICMP 协议号。最好的方法是在连接数据服务器的端口上过滤掉由服务器发出的 ICMP 回应包。这就起到了实现 ICMP 单向访问了。

2）配置步骤：

```
Switch# access-list 300 deny icmp host 192.168..4.1 any echo-reply
Switch# access-list 300 permit ip any any
```

并且要把这个访问控制列表应用到连接数据服务器的端口（本例为 port1/1）

```
Switch# port 1/1
Switch(port 1/1)# acl-filter 300
Switch# show access-list 300

 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

 Extended IP access list:
  GroupId 300 : reference count(1)
```

```
R 1 deny icmp SI 192.168.4.1 DI any echo-reply Active
R 2 permit SI any DI any Active
```

```
Switch# show acl-filter

ACL group and Port Configuration Information
port            groupId              status
1/1              300                  Active
```

4.扩展 IP 规则的 acl（单向 TCP 连接访问控制实例）



1） 网络环境：

为了防止一般网络用户主动连接到重要部门的网络，而仅仅允许重要部门可以主动发起到一般网络用户的联接，这就需要用到单向 TCP 连接。最好的方法是在连接一般网络用户的端口上过滤掉由一般用户发起的 TCP 连接。（本案例中，假设一般用户的网络连接到 iSpirit4504 交换机的 1/1 端口，重要部门的用户连接到其它端口）

2）配置步骤：

```
Switch# access-list 200 deny tcp any any 0 syn 1 ack 0
Switch# access-list 200 permit ip any any
```

并且要把这个访问控制列表应用到 1/1 端口

```
Switch# port 1/1
Switch(port 1/1)# acl-filter 200
```

3）查看配置信息

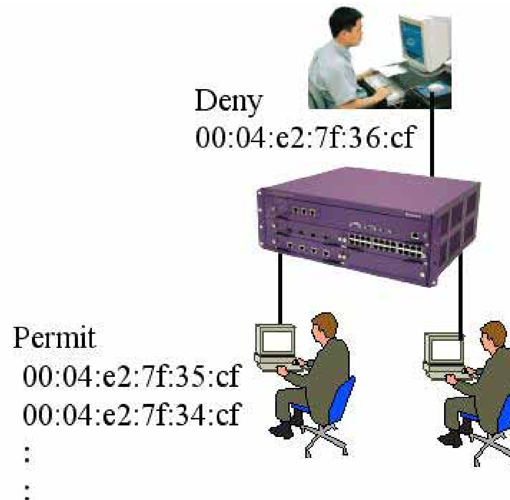
```
Switch# show access-list
 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.
 Extended IP access list:
  GroupId 200 : reference count(1)
   R 1 deny tcp SI any DI any syn 1 ack 0 Active
   R 2 permit SI any DI any Active
```

```
Switch# show acl-filter
ACL group and Port Configuration Information
port             groupId              status
1/1               200                  Active
```

5.MAC 地址规则的访问控制列表

1） 网络需求：

基于安全的考虑，控制 mac 地址为 00:04:e2:7f:36:cf 的特定用户（本例中用户连接到 iSpirit4504 的 1/1 端口）的数据流不能通过交换机进行转发，而允许其它 mac 地址的数据流通过。



2）配置步骤：

A ．建访问控制列表

Switch# access-list 400 deny 0 ip 00:04:e2:7f:36:cf　　//这里的 0 表示所有 vlan。Ip 表示网络协议

Switch# access-list 400 permit 0 ip any　　//0 和 ip 的所表示的意义同上。Any 表示任何 mac

B. 把访问控制列表应用到 iSpirit4504 的 1/1 端口上对流入的数据流做控制

Switch# port 1/1

Switch(port 1/1)# acl-filter 400

C.查看配置信息

Switch# show acl-filter

ACL group and Port Configuration Information

module/port	groupId	status
1/1	400	Active

Switch# show access-list 400

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type

SP - Source Port, DP - Destination Port, PT - Protocol Type

```
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

MAC address list:
 GroupId 400 : reference count(0)
  R 1 deny ip SM 00:04:e2:7f:36:cf DM any Active
  R 2 permit ip SM any DM any Active
```

3) 排错：

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表。还需要用 show access-list 命令来进行查看访问控制列表配置是否正确。

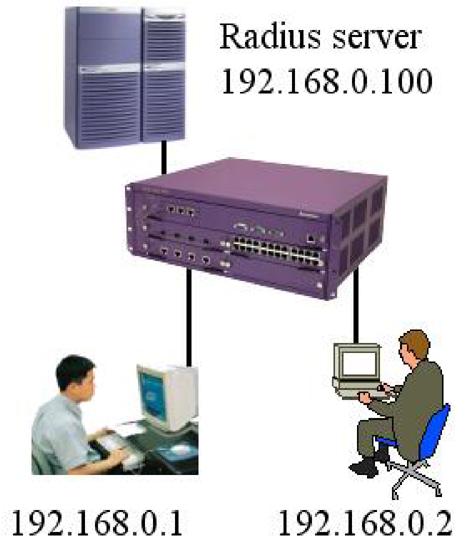
注意 mac 地址一定要书写正确，否则将不起任何作用。而且默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

//注意：以上 acl 的配置实例都是在 4 端口模块下进行配置的。如果要在 24 端口模块下也要使用 acl，那么必须在 24 端口模块下也配置 acl。

十五. 802.1x 认证

1. 网络需求

iSpirit4504 交换机放置了 radius 服务器，ip 地址为 192.168.0.100，子网掩码为 255.255.255.0；用户的 ip 地址为 192.168.0.1 ～ 192.168.0.3，子网掩码为 255.255.255.0。为了控制非法用户使用网络，需要在 iSpirit4504 交换机上打开 802.1x 认证机制，在用户使用的 pc 机上安装 802.1x 客户端，用户只有输入正确的用户名和密码并通过 radius 服务器认证，才能访问网络，用户的数据才能被交换机进行路由和转发。网络拓扑图如下：



2.配置步骤

1）在全局模式下打开 802.1x 的认证进程，

Switch# dot1x

2） 打开特定端口为 802.1x 的认证端口，本例以端口 1 为例子。

Switch# dot1x control auto 1/1 // 1/1 为端口号，如果还有其它端口要对接入的用户进行 802.1x 的认证，那么只要在这个命令上改一下端口号就可以。

3）指定 radius 服务器的 ip 地址

Switch# radius-server host 192.168.0.100

4）配置和 radius 服务器相匹配的认证密匙。根据实际情况要和 radius 所配置的一致

Switch# radius-server key radiuslenovonetworks

5）查看 802.1x 是否配置正确

```
Switch# show dot1x
Global 802.1X Parameters
 Dot1x Status          :        Enable    //全局模式下，已经启用了 802.x 认证
 ReAuth-enabled        :        no
 Accounting-enabled    :        yes
```

```
 ReAuth-period          :          3600
 Quiet-period           :          60
 Tx-period              :          30
 Server-timeout         :          10
 Max-req                :          3
 reAuthMax              :          3

 802.1X Port Summary
 PortName   Status       Mode     HostNum
1/1          Link Down   auto       100     //本例中，已经在端口 1 启用 802.1x 认证
1/2           Link Down    n/a        100
1/3           Link Down    n/a        100
```

查看 1/1 端口的状态

```
Switch# show dot1x 1
 Port-control              : auto
 Maximum hosts             : 250
 Current Connecting hosts : 0
```

查看所配置的 radius 服务器是否正确

```
Switch# show radius-server
 PrimaryServerIp   : 192.168.0.100
 OptionServerIp    : 0.0.0.0
 UdpPort           : 1812
 accountingPort    : 1813
 ShareKey          : radiuslenovonetworks
 Vendor            :
 NasPort           : 0xc353
 NasPortType       : 0x0f
 NasPortServer     : 0x02
```

//如果要在 24 端口模块下也请用 802.1x,那么就要对 24 端口模块进行配置。配置方法与上述类似。

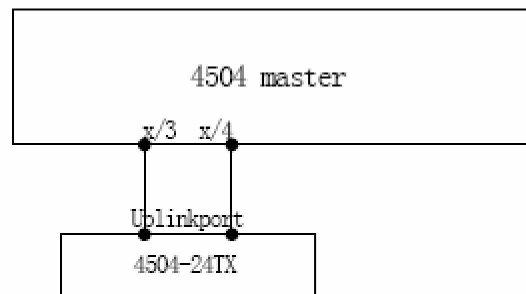
3.排错

1） 确认一定要打开 802.1x 的认证进程，用 show dot1x 命令
2） 确认打开特定的交换机端口做为认证端口，用 show dot1x 端口号
3） 正确配置 radius 服务器的 ip 地址和认证密钥，用 show radius-server 命令查看

附件 1：百兆模块的使用方法

当百兆模块插在某一个插槽时，主控板插槽的3,4端口就和百兆模块的上连端口（百兆模块的这两个端口在以后的配置介绍中，都称之为级连端口）相连接。在结构上百兆模块像一个独立二层交换机。

百兆模块和 4504 主控板的结构如下图：



4504-24TX 结构图

百兆模块在 iSpirit4504 中是一个功能相对独立的模块，它有包含了独立的 VLAN，组播，igmp snooping 协议等二层的协议和功能。因此对百兆模块的单独管理非常重要。

当百兆模块为出厂配置时，系统会根据所插槽的槽号自动分配一个 IP 地址给当前这个模块。在主控板上可以通过 show 命令获取到插在当前插槽的模块的 IP 地址，也可以在主控板上配置这个 IP 地址。IP 地址配置成功后，以后对百兆模块的管理就可以通过这个 IP 地址进行。

通过主控获取百兆模块的 IP 地址后。可以通过 TELNET，WEB，SNMP 访问百兆模块，也可以通过主控直接登陆到百兆模块管理。

通过 TELNET，WEB，SNMP 访问百兆兆模块和普通的交换机管理类似，下面主要介绍从主控

上配置百兆模块的管理方式。

当一个百兆模块插在第 3 个槽时,在主控板上可以通过 slot 3 命令进入模块 3 的配置模式，在这个配置模式下，可以修改百兆模块的 IP 地址，显示百兆模块的 IP 地址，重启百兆模块，登录到百兆模块进行其他的配置。

附件 2：配置超级终端

1） 将交换机背后的串口与计算机的串口（com1/com2）用串口线连接起来。

2） 打开计算机按照图 1 打开超级终端



图 1 打开超级终端

3） 按图 2，3， 4 配置超级终端


新建连接 - 超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)
连接描述
新建连接
输入名称并为该连接选择图标:
名称(N):
test
图标(I):
确定
取消
断开
自动检测
自动检测
SCROLL
CAPS
NUM
捕
打

图 2

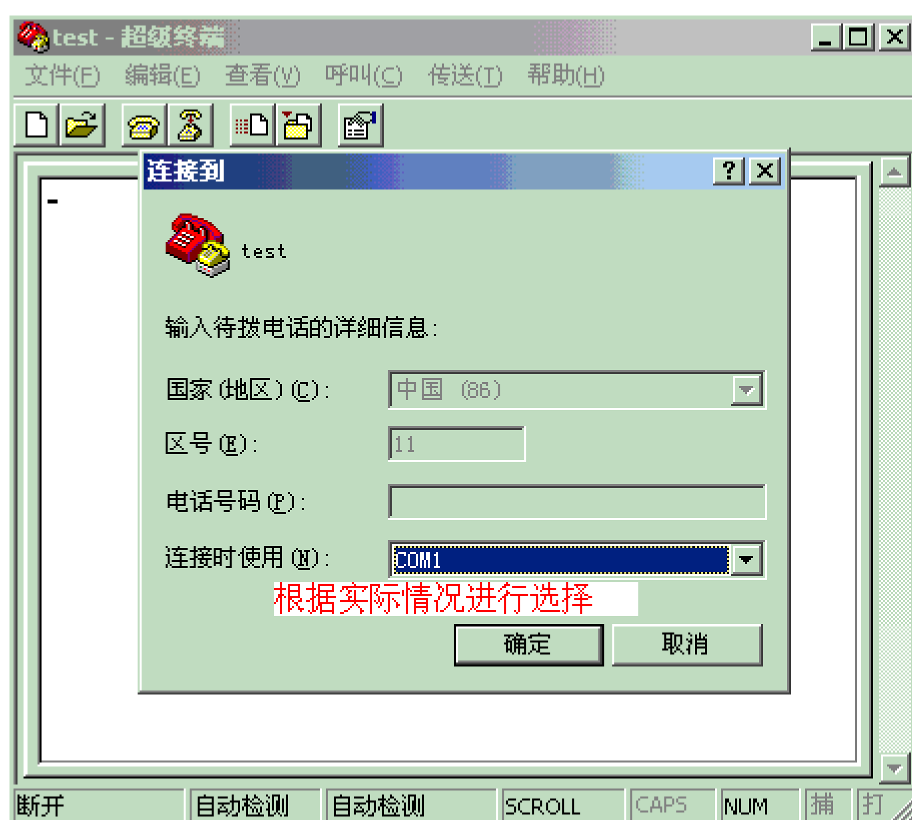

test - 超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)
连接到
test
输入待拨电话的详细信息:
国家(地区)(C):
中国 (86)
区号(E):
11
电话号码(P):
连接时使用(N):
COM1
根据实际情况进行选择
确定
取消
断开
自动检测
自动检测
SCROLL
CAPS
NUM
捕
打

图 3

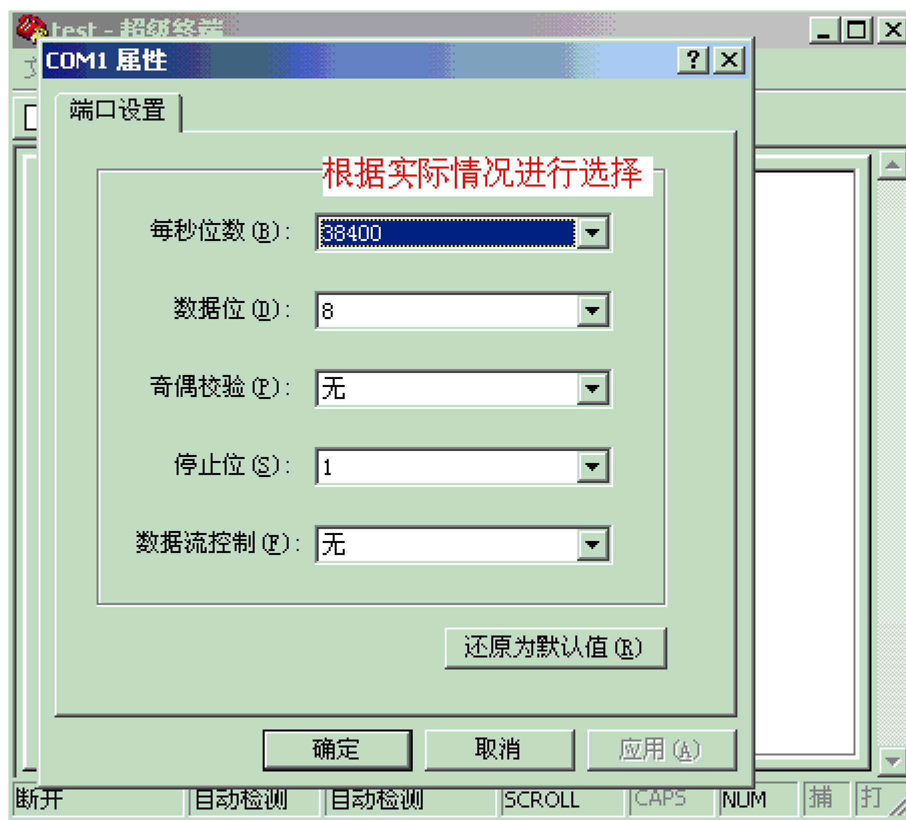


图 4

4）点击确定，就可以连接到交换机的 CLI 管理界面。